

REMARKS

This is responsive to the office action dated July 29, 2005. By this Response, claims 1, 3, 5 and 7 are amended. No new matter is introduced. Claims 1-8 are active for examination. A petition for a two-month extension of time is submitted concurrently herewith.

The Office Action rejected claims 1-8 under 35 U.S.C. §103(a) as being unpatentable over an internet document RFC 2630 (www.faqs.org/rfcs/rfc2630.html) and a 1999 literature document by Keutzer. The obviousness rejection is respectfully overcome because RFC 2630 and Keutzer cannot support a prima facie case of obviousness.

Claim 1, as amended, describes a storage medium that outputs information encrypted using a pre-stored encryption key. The encryption key is encoded using another encryption key that is part of a pair of asymmetrical keys, unique to, and held in secret in, the storage medium (such as encryption keys 205a and 205b in Fig. 3). Both the encoded information and the encoded encryption key are output from the storage medium. Appropriate support for the amendment can be found in, for instance, Fig. 3 and paragraphs [0038], [0046] and [0047] of the written description, which was published as U.S. Patent Application Publication No. US 2002/0034306.

In contrast, RFC 2630, the main document relied upon by the Office Action, describes encoding information using encryption keys and transmitting the encoded information. However, RFC 2630 does *not* specifically describe that *the encryption key* used in encoding the information is *further encoded using another encryption key that is part of a pair of asymmetrical encryption keys* that are *unique to, and stored in secrecy in*, the storage medium. RFC 2630 also *fails* to describe that the encoded encryption key is sent with the information that is encrypted using the encryption key. Therefore, RFC 2630 fails to describe that “when outputting information stored

inside said storage device to outside said storage medium, the information is encoded by using said encryption key, said encryption key is encoded using another encryption key that is part of a pair of asymmetrical keys unique to, and held in secret in, said storage medium,... and both said encoded information and said encoded encryption key are output,” as described in claim 1.

The other cited document, Keutzer, was relied on by the Office Action mainly for its purported teaching about integrating semiconductor segments, and fails to alleviate the deficiencies of RFC 2630.

Accordingly, RFC 2630 and Keutzer, even if combined, do not disclose every limitation of claim 1, and hence cannot support a prima facie case of obviousness. The obviousness rejection of claim 1 is untenable and should be withdrawn. Favorable reconsideration of claim 1 is respectfully requested.

Claim 2 depends on claim 1 and incorporates every limitation thereof. Consequently, claim 2 also is patentable over RFC 2630 and Keutzer by virtue of its dependency from claim 1. Favorable reconsideration of claim 1 is respectfully requested.

Independent claim 3, as amended, describes a storage medium that outputs information encrypted using a pre-stored encryption key. The encryption key is encoded by using another encryption key that is part of a pair of asymmetrical keys unique to, and held in secret in, the storage medium. Only the encoded information is output by the storage medium. When a signal showing that the encoded information is received by an external apparatus, the encoded encryption key is output after voiding the information stored in the storage device. Appropriate support for the amendment can be found in, for example, Fig. 6 and paragraphs [0068]-[0070] and [0072]-[0074] of U.S. Patent Application Publication No. US 2002/0034306.

As discussed earlier relative to claim 1, RFC 2630 and Keutzer, if combined, do not disclose further encrypting an encryption key that is used in encoding information by utilizing another encryption key that is part of a pair asymmetrical encryption keys unique to, and is stored in secret in, the storage medium. Furthermore, neither RFC 2630 nor Keutzer describes that, responsive to a signal showing that the encoded information is received by an external apparatus, the encoded encryption key is output after voiding the information stored in said storage device. Accordingly, RFC 2630 and Keutzer, even if combined, do not disclose “when outputting information stored inside said storage device to outside said storage device: the information is encoded using said encryption key, said encryption key is encoded by using another encryption key that is part of a pair of asymmetrical keys unique to, and held in secret in, said storage medium,...and when a signal showing that the encoded information is received by an external apparatus, said encoded encryption key is output after voiding said information stored in said storage device,” as recited in claim 3. Therefore, claim 3 is patentable over RFC 2630 and Keutzer, either combined or alone. Favorable reconsideration of claim 3 is respectfully requested.

Claim 4 depends on claim 3 and incorporates every limitation thereof. Consequently, claim 4 also is patentable over RFC 2630 and Keutzer by virtue of its dependency from claim 3. Favorable reconsideration of claim 4 is respectfully requested.

Independent claim 5, as amended, describes encoding information to be sent from a storage medium to an apparatus external to the medium, by utilizing a pre-stored encryption key. The encryption key is encoded utilizing another encryption key that is part of a pair of asymmetrical keys unique to, and held in secret in, the storage medium. The encoded information and the encoded encryption key are sent to, and stored in, the external apparatus,

Application No.: 09/943,754

without the another encryption key. Appropriate support for the amendment can be found in, for example, Fig. 3 and paragraphs [0038], [0046] and [0047] of U.S. Patent Application Publication No. US 2002/0034306.

As pointed out earlier relative to claim 1, RFC 2630 and Reutzer, combined, do not disclose that *the encryption key* used in encoding the information is *further encoded using another encryption key that is part of a pair of asymmetrical encryption keys* that are *unique to, and stored in secrecy in*, the storage medium, and that the encoded encryption key is sent with the information that is encrypted using the encryption key, as described in claim 5. Accordingly, claim 5 is patentable over the combination of RFC 2630 and Reutzer. Favorable reconsideration of claim 5 is respectfully requested.

Claim 6 depends on claim 5 and incorporates every limitation thereof. Consequently, claim 6 also is patentable over RFC 2630 and Keutzer by virtue of its dependency from claim 5. Favorable reconsideration of claim 6 is respectfully requested.

Independent claim 7, as amended, describes encoding information to be sent from a storage medium to an apparatus external to the medium, by utilizing a pre-stored encryption key. After receiving a signal showing that the encoded information is received by the external apparatus, the information stored in the storage device is voided. An encoded encryption key that is generated by encoding the encryption key using another encryption key that is part of a pair of asymmetrical keys unique to, and held in secret in, the storage medium, is sent to the external apparatus. Appropriate support for the amendment can be found in, for example, Fig. 6 and paragraphs [0068]-[0070] and [0072]-[0074] of U.S. Patent Application Publication No. US 2002/0034306.

As discussed relative to claims 1 and 4, RFC 2630 and Keutzer, even if combined, do not disclose further encrypting an encryption key that is used in encoding information by utilizing another encryption key that is part of a pair asymmetrical encryption keys unique to, and is stored in secret in, the storage medium. Furthermore, neither RFC 2630 nor Keutzer describes that, responsive to a signal showing that the encoded information is received by an external apparatus, the encoded encryption key is output after voiding the information stored in said storage device. Accordingly, RFC 2630 and Keutzer do not disclose that “information to be sent to said external apparatus is encoded utilizing said encryption key, and after receiving a signal showing said encoded information is received by said external apparatus, said information stored in said storage device is voided, and an encoded encryption key that is generated by encoding the encryption key using another encryption key that is part of a pair of asymmetrical keys unique to, and held in secret in, said storage medium, is sent to said external apparatus,” as recited in claim 7. Therefore, claim 7 is patentable over RFC 2630 and Keutzer, either combined or alone. Favorable reconsideration of claim 7 is respectfully requested.

Claim 8 depends on claim 7 and incorporates every limitation thereof. Consequently, claim 8 also is patentable over RFC 2630 and Keutzer by virtue of its dependency from claim 7. Favorable reconsideration of claim 8 is respectfully requested.

CONCLUSION

In light of the amendments and remarks above, it is submitted that this application is in condition for allowance. If there are any questions regarding this amendment or the application in general, a telephone call to the undersigned would be appreciated to expedite the prosecution of the application.

Application No.: 09/943,754

To the extent necessary, if any, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Wei-Chen Nicholas Chen
Registration No. 56,665

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 WNC:ct
Facsimile: 202.756.8087
Date: December 27, 2005

**Please recognize our Customer No. 20277
as our correspondence address.**